Svet
Evropske unije

Bruselj, 20. april 2023
(OR. en)

8512/23
ADD 1

Medinstitucionalna zadeva:
2023/0109 (COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	19. april 2023
Prejemnik:	Thérèse BLANCHET, generalna sekretarka Sveta Evropske unije
Št. dok. Kom.:	COM(2023) 209 final - Annex
Zadeva:	PRILOGA k UREDBI EVROPSKEGA PARLAMENTA IN SVETA o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje

Delegacije prejmejo priloženi dokument COM(2023) 209 final - Annex.

Priloga: COM(2023) 209 final - Annex

EVROPSKA
KOMISIJA

Strasbourg, 18.4.2023
COM(2023) 209 final

ANNEX

PRILOGA

k

UREDBI EVROPSKEGA PARLAMENTA IN SVETA

o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje

PRILOGA

Uredba (EU) 2021/694 se spremeni:

(1) v Prilogi I se oddelek/poglavje „Specifični cilj 3 – kibernetska varnost in zaupanje“ nadomesti z naslednjim:

„Specifični cilj 3 – kibernetska varnost in zaupanje

Program spodbuja krepitev, razvoj in pridobivanje osnovnih zmogljivosti za zaščito digitalnega gospodarstva, družbe in demokracije v Uniji s krepitvijo industrijskega potenciala in konkurenčnosti Unije na področju kibernetske varnosti ter z izboljšanjem zmogljivosti zasebnega in javnega sektorja za zaščito državljanov in podjetij pred kibernetskimi grožnjami, vključno s podporo pri izvajanju Direktive (EU) 2016/1148.

Začetni in po potrebi poznejši ukrepi v okviru tega cilja vključujejo:

1. Sovlaganje držav članic v kibernetskovarnostno napredno opremo, infrastrukture ter tehnične izkušnje, ki so ključnega pomena za zaščito kritičnih infrastruktur in digitalnega enotnega trga na splošno. Tako sovlaganje lahko vključuje naložbe v zmogljivosti za razvoj kvantnih tehnologij in podatkovne vire za kibernetsko varnost, situacijsko zavedanje v kibernetskem prostoru, ***vključno z nacionalnimi centri za varnostne operacije in čezmejnimi centri za varnostne operacije, ki sestavljajo evropski kibernetski ščit***, ter druga orodja, ki se dajo na voljo javnemu in zasebnemu sektorju po vsej Evropi.

2. Obsežnejši razvoj obstoječih tehnoloških zmogljivosti in mreženje strokovnih centrov držav članic ter zagotavljanje, da se te zmogljivosti odzivajo na potrebe javnega sektorja in industrije, vključno z izdelki in storitvami, ki krepijo kibernetsko varnost znotraj digitalnega enotnega trga.

3. Zagotavljanje široke uvedbe učinkovitih najsodobnejših rešitev za kibernetsko varnost in zaupanje v vseh državah članicah. Taka uvedba vključuje krepitev zanesljivosti in varnosti izdelkov, od njihovega oblikovanja do trženja.

4. Podpora zapolnjevanju vrzeli v veščinah glede kibernetske varnosti, na primer z usklajevanjem programov za razvoj takih veščin, njihovo prilagajanje specifičnim sektorskim potrebam in olajšanje dostopa do specializiranih, ciljno usmerjenih usposabljanj.

5. ***Spodbujanje solidarnosti med državami članicami pri pripravi na pomembne kibernetskovarnostne incidente in odzivanju nanje z uvedbo čezmejnih storitev kibernetske***

varnosti, med drugim s podporo za medsebojno pomoč med javnimi organi in vzpostavitvijo rezerve zaupanja vrednih ponudnikov kibernetskovarnostnih storitev na ravni Unije.“;

(2) v Prilogi II se oddelek/poglavje „Specifični cilj 3 – Kibernetska varnost in zaupanje“ nadomesti z naslednjim:

„Specifični cilj 3 – Kibernetska varnost in zaupanje

3.1 Število skupno naročenih infrastruktur ali orodij za kibernetsko varnost ali obojega[1]

3.2 Število uporabnikov in uporabniških skupnosti, ki imajo dostop do evropskih zmogljivosti za kibernetsko varnost

3.3 Število ukrepov za podporo pripravljenosti in odzivanju na kibernetskovarnostne incidente v okviru mehanizma za izredne kibernetske razmere“.

PRILOGA […]